In re Patent Application of:
POMET ET AL.
Serial No. **09/727,300**
Filing Date: **NOVEMBER 30, 2000**

REMARKS

Applicants would like to thank the Examiner for the thorough examination of the present application. The arguments supporting patentability of the claims are presented in detail below.

I. The Claimed Invention

The present invention, as recited in independent Claim 12, for example, is directed to an electronic device comprising a central processing unit, at least one peripheral device, and a data bus connected between the at least one peripheral device and the central processing unit through which data travels at a rate of a clock signal. The electronic device further comprises a transmission line connected between the at least one peripheral device and the central processing unit for providing a random signal thereto that is synchronous with the clock signal. The central processing unit and the at least one peripheral device each comprises a data encryption/decryption cell connected to the data bus and to the transmission line for generating a same current secret key at each clock cycle based upon the random signal.

The data encryption/decryption cell in the central processing unit and in the at least one peripheral device advantageously makes the electronic device more secure by making it more difficult to determine the data elements that travel through the data bus when an intruder observes current consumption of the electronic device.

Independent device Claim 25 is similar to independent device Claim 12 except the at least one peripheral device has been changed to at least one memory device. Independent device Claim 34 is similar to independent device Claim 12 except this claim is directed to a smart card. Independent method Claim 42 is similar to independent device Claim 12.

II. The Claims Are Patentable

The Examiner rejected independent Claims 12, 25, 34 and 42 over the Carmeli patent. The Carmeli patent discloses a system for providing a trusted computer communication network including a master decision maker unit coupled to the trusted network, and at least one slave communication unit coupled to the master unit by a wide bus connection that has multiple unidirectional communication channels, and connected to a non-trusted network. The trusted network is physically isolated at all times from the non-trusted network, and all data transported between the trusted network and the non-trusted network is transported between the master unit and the slave unit.

The Examiner has taken the position that the claimed invention is disclosed in the following sections of the Carmeli patent: column 5 line 65 to column 6, line 18 (CPU and at least one peripheral device); column 9, lines 13-25 (data bus connected between the at least one peripheral device and the central processing unit through which data travels at a rate of a clock signal, and a transmission line connected between the at least one peripheral device and said central processing unit for providing a random signal thereto that is synchronous with the

clock signal); and column 9 line 54 to column 10, line 12 (the CPU and the at least one peripheral device each comprising a data encryption/decryption cell connected to the data bus and to the transmission line for generating a same current secret key at each clock cycle based upon the random signal).

More particularly, the Examiner has characterized the master unit 16 and one of the slave units 18 as the CPU and the at least one peripheral device. As shown in FIG. 3 in Carmeli, a master unit 16 or a slave unit 18 comprises a single board computer SBC 22 that is connected to a wide bus gate card 24 via a computer bus 28. Carmeli discloses that the internal data exchanges on the bus 28 between the SBC 22 and the wide bus gate card 24 within a master or slave unit 16, 18 are protected via a secret key signature of the transmitted data on the bus (column 8, line 50 and on).

Carmeli further discloses that a common secret key, which changes periodically, is known by the SBC 22 and by the wide bus gate card 24 (column 8, lines 46-49). The SBC 22 and the wide bus gate card 24 thus use the same temporary secret key at the same time to sign the data exchanged between them (column 9, lines 14-15). Furthermore, the common secret key is produced locally by each of the SBC 22 and the wide bus gate card 24 by using values that are randomly generated (column 9, lines 18-20).

However, in accordance with the claimed invention, the processor and the at least one peripheral device each comprises a data encryption/decryption cell using the same secret key, with a current value of this secret key being produced locally at each

clock cycle based upon a random signal which is synchronous with the clock signal, and which is applied to each cell by a transmission line. The transmission line is distinct from the data bus.

The transmission line in the claimed invention, which is connected between the processor and the at least one peripheral device, provides a synchronous random signal to the processor and the peripheral device, and from which each one produces locally the same value of the secret key, wherein the secret key is used to secure data exchanges between them.

In other words, the data bus and the transmission line are separated from one another, as best shown in FIG. 2 in the Applicants' application. Carmeli fails to provide this noted distinction. Reference is directed to column 7, lines 52 to 63 of Carmeli, which provides:

> "The standard computer communication network, whether it is the hostile or the trusted net, is always connected to the SBC. Units exchange data through the wide bus gate card, and only through these sections. The internal communication between the SBC and the wide bus gate cards is done through a standard computer 28 (shown in FIG. 3), which may be, for example, a PCI or ISA bus. The SBC can freely write data to the wide bus gate card, but does not have direct access to the wide bus." (Emphasis added).

Contrary to the assertion of the Examiner, no transmission line, distinct from the computer bus 28, can be

identified in the slave or master unit of Carmeli between the SBC 22 and the wide bus gate card 24, which could be used to provide a synchronous random signal to each section 22 and 24 or the master or slave unit for the production of the common secret key.

In addition, Carmeli teaches that the random values used to produce the secret key are generated by the wide bus gate card 24 at the time of starting, and that these values are transmitted on the computer bus 28 to the SBC 22. Reference is directed to column 9, lines 32 to 42 of Carmeli, which provides:

> "The permanent values are randomly generated by the wide bus gate card at startup time. Since, at that time, the system (i.e., the hardware described above) is physically disconnected from both networks, it is safe to send these values to the SBC through the computer bus. In addition, the wide bus gate card generates another number which is considered as the current secret key number, and it sends that number to the SBC, right after the permanent values. Now, both sections are synchronized: both use the same function (because they use the same permanent values) and both start from the same initial value of a secret key." (Emphasis added).

Consequently, the two sections 22 and 24 are synchronized and can produce the same secret key starting from these exchanged random values. The Applicants submit that Carmeli fails to disclose a transmission line distinct from the bus 28 that is used to transmit a synchronous random signal to each

section 22, 24, from which the common secret key would be produced. On the contrary, the random values used to produce the secret key common to each section are transmitted on the computer bus at the time of starting.

Furthermore, according to the claimed invention, the processor and the peripheral device locally produce a current value of the secret key at each cycle of clock from the random signal synchronous of the clock signal. In sharp contrast, Carmeli discloses the current value of the secret key is modified on randomly generated request (column 9, lines 50-53). The modification of the current value of the secret key is thus not controlled by the clock signal contrary to the claimed invention.

Accordingly, it is submitted that independent Claim 12 is patentable over the Carmeli patent. Independent Claims 25, 34 and 42 are similar to independent Claim 12. It is submitted that these independent claims are also patentable over the Carmeli patent. In view of the patentability of independent Claims 12, 25, 34 and 42, it is submitted that the dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed

In re Patent Application of:
POMET ET AL.
Serial No. **09/727,300**
Filing Date: **NOVEMBER 30, 2000**

below.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330

CERTIFICATE OF FACSIMILE TRANSMISSION

I HEREBY CERTIFY that the foregoing correspondence has been forwarded via facsimile number 571-273-8300 to the Commissioner for Patents on this 15 day of March, 2007.